PRICEWATERHOUSECOOPERS

An Overview of HIPAA's Applicability to Employers, and of Employer Responses
(Beyond Fear and Loathing)

Jon Neiditz
October, 2002

HIPAA's Provisions

- Group and individual insurance reform, tax–related health provisions, fraud and abuse
- Administrative simplification
  - Create **standards** for the electronic transmission of certain health care transactions to improve the efficiency and effectiveness of the healthcare system
  - To enhance public trust in a standardized system, must protect the **privacy** and **security** of an individual's health information
- Compliance dates for administrative simplification
  - Transaction standards – October 16, 2003, with a filing for an extension due by October 15, 2002
  - Privacy rules – April 14, 2003; no sign that any change is possible; privacy is the lion's share of the work for most employers that are not self-administered
  - Security requirements – proposed regulations (final rule may be issued in 2002)

Transaction Provisions

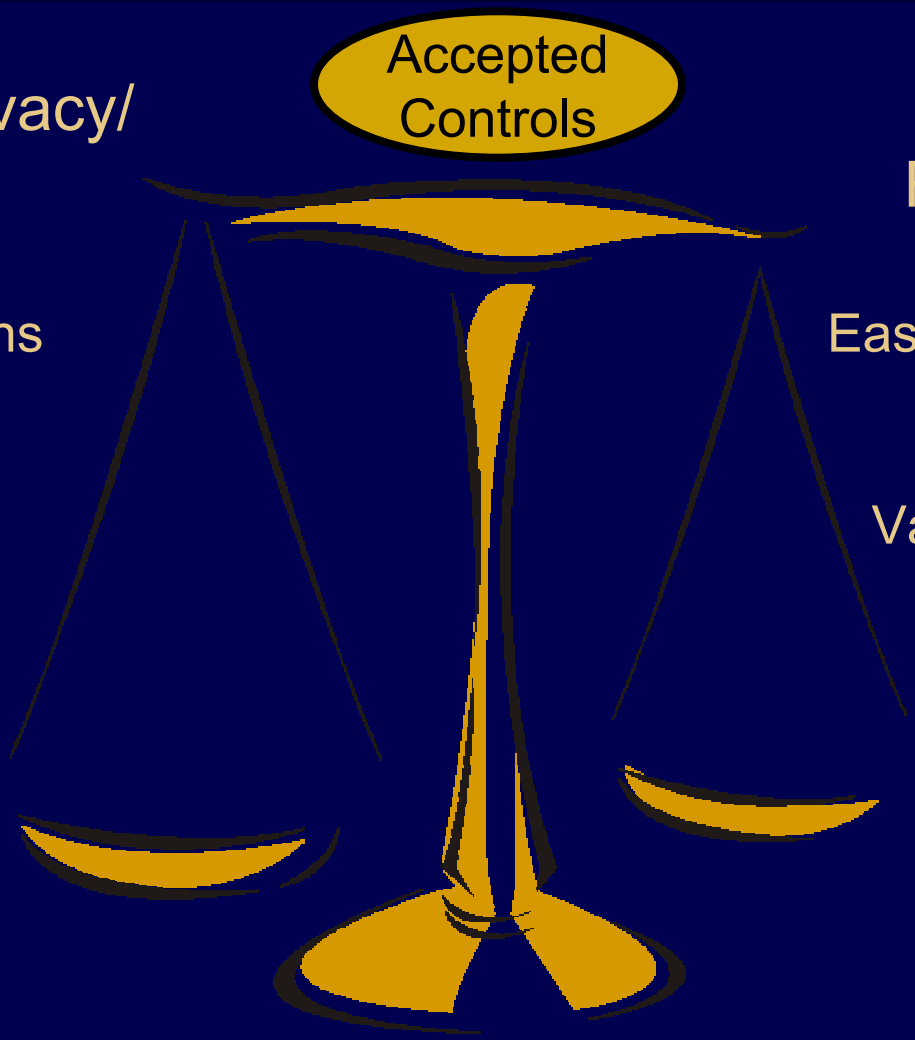
Providers	Challenges for the Self-Administered	Payors	Opportunities for Other Employers	Sponsors
FUNCTIONS		**FUNCTIONS**		**FUNCTIONS**
Eligibility Verification	270 (Eligibility Inquiry) → 271 (Eligibility Information) ←	Enrollment	834 (Benefit Enrollment & Maintenance) ←	Enrollment
Pre–Authorization and Referrals	278 (Referral Authorization and Certification) ↔ 148 (First Report of Injury)* →	Pre–Certification & Authorization		
Service Billing Claim Submission	837 (Claims Submission) → 275 (Claims Attachment)* →	Claims Acceptance	270 (Eligibility Inquiry) ← 271 (Eligibility Information) →	
Claims Status Inquiries	276 (Claim Status Inquiry) → 277 (Claim Status Response) ←	Claims Adjudication		
Accounts Receivable (AR)	835 (HealthCare Claim Payment Advice) ←	Accounts Payable	811 (Invoice)* → 820 (Payment Order/RA) ←	

** Note: These are not contained in the initial Transactions and Code Sets Final Rule*

Balancing Priorities

Information Privacy/
Security Risks

Employee Relations
Media Exposure
Civil Liability
Compliance Risks
Contractual Risks



Business
Requirements

Ease of Administration
Cost Containment
Productivity
Valuable Information
Labor Relations

HIPAA Privacy Rule: Key Provisions

- General Requirements
- Special Rules for Group Health Plans
- Firewalls
- Covered Entities
- Protected Health Information
- Use and Disclosure Rules
- Individual Rights
- Business Associates
- Training Requirements

General Requirements

- **Protecting records** containing individually identifiable health information so that they are not available to those who do not need them.
- **Separating plan administration from other HR functions**, changing plan documents accordingly, and certifying compliance to vendors.
- Providing **information to employees** about their privacy rights and how their information can be used or disclosed.
- Developing and adopting clear **privacy procedures**, and **training** employees on them.
- Designating a **privacy official** to be responsible for seeing that the privacy procedures are adopted and followed.
- Identifying and agreeing to the required contractual provisions with all **business associates**, and taking action if violations become known.
- Establishing processes for information **access** to and **amendment** of protected information**,** and **accounting** for non-exempt disclosures.
- Providing **complaint and remediation** mechanisms and processes.

Special Rules for Group Health Plans

- Generally, the plan sponsor may only receive information from the group health plan or its vendors to carry out "plan administration functions" if it:
  1) modifies its plan documents
  2) places the proper controls on the flow of PHI, and
  3) issues a certification to the group health plan about the protections applied to the information.
- "Plan administration functions" do not include employment–related functions or functions related to other plans.
- Amendments and certifications must:
  - Establish uses and disclosures of PHI by the plan sponsor and its agents, and
  - Ensure adequate separation between group health plan and plan sponsor, in part by describing those employees or groups controlled by the plan sponsor to be given access to PHI, and restricting their access and use.
- If a plan sponsor does not make the required changes in its documents and practices and does not certify that it has done so, it may only receive "summary" information from its vendors, and only in the context of premium bids and of modifying, amending or terminating the plan.

A Privacy Advocate's View of an Employer

HMO/ Insurer

Employer Group Health Plan Function

Plan Sponsor Function

Employer HR/Mgmt Function

Covered Entities

Non–Covered Entities

What is a Group Health Plan?

Covered Benefit Plans

- Medical Benefit Plans
- Long Term Care
- Dental Plans
- Vision Plans
- Prescription Drug Plans
- Many Employee Assistance Programs (EAPs)
- Flexible Spending Accounts
- Personal Health Accounts
- Some Executive Physical Programs

Excluded (though impacted)

- Life Insurance
- Workers' Compensation
- AD&D
- STD and LTD
- Auto Insurance
- Reinsurance/Stop Loss
- Other Property/Casualty

Protected Information

Protected Health Information (PHI)

- Any information that relates to:
  - Past, present, or future health or condition (physical or mental);
  - Provision of health care; or
  - Past, present, or future payment for the provision of healthcare.
- Which identifies or could be used to identify an individual.
- "CREATED OR RECEIVED BY A COVERED ENTITY OR EMPLOYER."
- Whether in electronic, printed, or spoken form.
- To not be PHI, there must be no reasonable basis to believe that the information can be used to identify an individual.
- For almost all employers' purposes, PHI has the same meaning as Individually Identifiable Health Information (IIHI).

Areas of Employer Risk and Attention

Health benefit plans are covered entities:

- change plan documents
- redefine access to and/or use of information within HR
- redefine access to and/or use of information by labor representatives

Very rarely, provider functions of an employer may be covered, but only if they engage in the standard transactions electronically:

- in-house EAPs
- onsite clinics/pharmacies
- occupational health programs
- other programs providing health services to employees

Review and possible modification of:

- Involvement of local human resources in benefits and other health advocacy
- health and productivity programs
- disease management/ intervention activities
- health promotion/disease prevention
- integrated disability programs
- disability investigations
- individual risk appraisals
- fitness–for–duty exams
- absenteeism studies
- workplace medical and safety surveillance
- union contracts and practices

Use and Disclosure of PHI, and the Minimum Necessary Standard

A covered entity may not use or disclose PHI except as permitted or required under the regulation.

- Permitted without obtaining a (very specific, time-limited and freely given) "authorization" from an employee:
  - Payment (e.g., eligibility or coverage determinations, claim adjudication, billing, obtaining reinsurance payments, medical necessity/coverage review)
  - Health care operations (e.g., underwriting, premium rating, etc. for creation, renewal, or replacement of a contract for insurance or benefits, conducting or arranging for medical review, legal services, and auditing functions)
  - Treatment
- Covered entities may use or disclose only the minimum amount of PHI that is reasonably necessary to achieve the purpose of the use or disclosure.
- For routine requests and disclosures, there must be policies and procedures designed to limit the disclosure of PHI to the amount and type reasonably necessary; case–by–case review is not necessary.

New Rights of Employees & Dependents

Individual rights → employer obligations and systems challenges

- Ensure **notification** of privacy rights, policies and procedures (very detailed notice requirements)
- Ensure individuals have **access** to their own PHI (designated record set)
- Allow **amendment** of PHI (designated record set)
  - May deny request but must then allow individual to place an explanation in the record
- Ensure individuals receive an **accounting** of non–exempt disclosures of PHI over the past six years (not limited to designated record set)
  - Excludes treatment, payment, health care operations
- Ensure individuals may request restrictions on use or disclosure of their PHI (though such requests need not be granted)
- Ensure communications are made by an alternative means or at alternative location when requested

Steps to an Optimal HIPAA and Privacy Implementation

- Begin with a careful covered entity analysis, drawing clear lines around those areas in which the detailed rules of HIPAA will apply, and those areas in which other privacy policy might apply.
- Never lose sight of what your key business associates are doing or failing to do about HIPAA and offering you (force them to be specific!), and of what other employers are doing about HIPAA.
  - Most employers should not have to build their own systems to perform the privacy administrative functions (or the eligibility/enrollment and premium transactions).
  - Employers will be judged on an emerging consensus about “reasonable” practical solutions for each of the many privacy and security standards.
- Business associates and other key vendors may need to be treated differently based on different types and levels of risk; seek indemnification from high-risk vendors.
- Perform assessment only to the extent necessary to define and accomplish necessary and appropriate projects; you do not need a regulatory audit!

Examples of Change Driven by HIPAA in Benefits and Human Resources

- Rethinking local HR's involvement in benefits advocacy and health issues
  - Does local HR represent the "plan sponsor" function?
  - Does it require the same level and type of training as the Benefits Department?
  - What access, if any, does it continue to have to information from the TPA?
  - If not HIPAA privacy, should broader privacy rules apply?
- The problem of the "coercive" health plan
  - EAPs as a duplicate mental health benefit AND management tool
  - Executive physicals
- Consolidation among TPAs, PBMs, disease management vendors, etc.
  - Can yours get specific about how it will do access, amendment, accounting and alternative addresses on your behalf?
  - Will it indemnify you (meaningfully) for failure to perform those functions or comply with your policies?
- Standard transactions and code sets provide a systems platform on which the number of benefits options can be expanded and options easily removed and added—cutting through delays in responding to demand and transaction costs associated with emerging models in health benefits.
- Do HIPAA privacy and security provide the right backbone of rights to justify the information transfers inherent in consumer-directed healthcare, genomics, e-health, and other trends?

Your worlds  Our people